REMARKS

Claim Status

Claims 1-32 are now pending, with claims 1 and 32 being in independent form. Claims 1, 3, 11, 13, 15, 17, 19, 20, 22, 23, 25-29 and 32 have been amended. The amendments to claims 3, 11, 13, 15, 17, 19, 20, 22, 23 and 25-29 correct minor wording of the claims, and are cosmetic in nature. No new matter has been added. Support for the amendment to independent claims 1 and 32 may be found, for example, at pg. 8, lines 14-16 of the specification as originally filed. Reconsideration of the application, as herein amended, is respectfully requested.

Overview of the Office Action

Claims 1-32 stand rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Pub. No. 2002/0129247 ("*Jablon*") in view of U.S. Patent No. 5,867,577 ("*Patarin*"), and further in view of EP 0 325 238 ("*Yeda*") and U.S. Pub. No. 2001/0016910 ("*Tanimoto*").

Claim 32 stands rejected under 35 U.S.C. §103(a) as unpatentable over *Jablon* in view of *Patarin*, and further in view of U.S. Pub. No. 2003/0182554 ("*Gentry*"), *Tanimoto* and *Yeda*.

Applicant has carefully considered the Examiner's rejections and the comments provided in support thereof. For the following reasons, Applicant respectfully asserts that all claims now presented for examination in the present application are patentable over the cited art.

Patentability of the Independent Claims 1 and 32 Under 35 U.S.C. §103(a)

Independent claim 1 has been amended to clarify that at least one pseudo-random number $\underline{r}$ is produced at the application before the hard-wired electronic chip is placed into circulation, parameters $\underline{x}$ corresponding to the at least one pseudo-random number $\underline{r}$ are calculated at the

application before the hard-wired electronic chip is placed into circulation, where each corresponding parameter x is linked to a pseudo-random number r by a mathematical relationship, and that the corresponding parameter x is stored in a data memory of the electronic chip before the hard-wired electronic chip is placed into circulation. Independent claim 32 has been correspondingly amended. The Examiner-applied combination of cited art fails to teach or suggest at least these express recitations of now-amended independent claims 1 and 32.

Jablon relates to a method for authenticating one party to the other using a series of messages that are exchanged over an open, insecure network, where interception or modification of the messages by an un-trusted third party may be possible (see Abstract). *Jablon* (paragraph [0040]) describes the establishment of "a large mutually-authenticated shared secret key between parties over an open insecure channel, where the authentication is based solely on mutual possession of a potentially small shared secret, such as a password".

As described at paragraph [0057] of *Jablon*, a pair of entities, i.e., Alice and Bob, "alone share knowledge of a secret password S". Bob proves his identity to Alice by proving his knowledge of the result of a key exchange protocol, which is determined by parameters set according to a function of S". This exchange is known in the art as a simple password-authenticated exponential key exchange (SPIKE).

In contrast, the claimed invention is directed to an asymmetrical cryptographic method and device for protecting a hard-wired electronic logic chip against fraud in transactions between the hard-wired electronic chip and an application. Consequently, the claimed invention provides an asymmetrical pair of keys comprised of a private key s and a public key p. In addition, the calculation of an authentication value V occurs within the hard-wired electronic chip using input

parameters that include a random number r. *Jablon* simply fails to teach or suggest anything even resembling the claimed invention.

With reference to Fig. 1, *Jablon* teaches that Q_A is computed by Alice at step 104, which is part of a sequence comprised of steps 103, 104 and 106, where the computed Q_A is then sent to Bob (see paragraph [0066]). Applicant's independent claim 1 recites the step of "producing, at the hard-wired electronic chip, the pseudo-random number r specific to the transaction via a serial pseudo-random generator included in the hard-wired electronic chip". *Jablon* fails to teach or suggest this limitation. Independent claim 1 additionally recites that the pseudo-random generator is "included in the hard-wired electronic chip"; the pseudo-random random number r is thus produced locally in the hard-wired electronic chip via the pseudo-random generator. Independent claim 32 recites a corresponding feature. In *Jablon*, however, the value of the random number R_A is chosen from between 1 and N, and N is actually known by Bob. Moreover, *Jablon* teaches that the random number calculated at Bob is R_B, which differs from R_A. *Jablon* thus fails to teach or suggest this claimed step of applicant's independent claims 1 and 32.

Independent claim 1 further recites the step of "sending from the hard-wired electronic chip to the application the parameter x calculated by the application prior to the transaction, which is linked to the pseudo-random number r by the mathematical relationship and stored in the data memory of the hard-wired electronic chip". Device claim 32 also recites a corresponding feature. *Jablon* fails to teach or suggest this claimed step, or the structure correspondingly recited in independent claim 32.

With further reference to Fig. 1 of *Jablon*, assuming *arguendo* that Q_A corresponds to the parameter x (recited in independent claims 1 and 32) that would be sent to Bob, where

$Q_A=H_{RA}(g)$, *Jablon* would still fail to teach or suggest applicant's claimed invention as recited in independent claims 1 and 32. Independent claims 1 and 32 recite that at least one parameter x is calculated by the application and is stored in the hard-wired electronic chip before the hard-wired electronic chip is placed into circulation. In *Jablon*, the parameter Q_A is not calculated by Bob before any sort of hard-wired chip is placed into circulation. Consequently, *Jablon* does not provide a pre-circulation calculation that provides a parameter x that was stored or could have been stored in an internal memory of Alice (e.g., the chip with continued reference to this construct). *Jablon* thus once again fails to teach or suggest the recited subject matter of independent claims 1 and 32.

Independent claim 1 additionally recites the step of "calculating, at the hard-wired electronic chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function whose input parameters are at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys". Independent claim 32 recites a corresponding limitation. *Jablon* also does not teach or suggest this step, or the corresponding limitation of independent claim 32.

Jablon teaches that Alice (e.g., the chip) calculates a parameter constituting the entire or a portion of the authentication value V. *Jablon* (paragraph [0068]) teaches that "After Alice receives Q_B from Bob 125, Alice computes $K=H_{RA}(Q_B)$ 105". *Jablon* (paragraph [0076]) additionally explains that "Alice constructs the proof 127, sends this proof in a message V_A to Bob 108, and Bob verifies the proof 127 against his known value for K". *Jablon* (paragraph [0076]) further explains that "Alice may construct V_A using a one-way function of the value of K, since K is a one-time randomly-generated large value". *Jablon* thus teaches that the verification value V_A is constructed as the result of a one-way function of K, which is itself the

result of a function whose input parameter is Q_B which is computed by Bob and sent to Alice from Bob.

In contrast, applicant's independent claims 1 and 32 recite that the authentication value is entirely or partly equal to the result of a serial function whose input parameters are at least the random number r and a private key s. *Jablon* fails to teach or suggest this recited feature of independent claims 1 and 32.

Moreover, independent method claim 1 recites the step of "verifying, at the application, said authentication value V via a verification function whose input parameters consist of public parameters including at least a public key p". *Jablon* also fails to teach or suggest this claimed step. As recited in claim 1, the input parameters of the verification function are public parameters. *Jablon*, on the other hand, teaches that the input parameter of verification function h(h) is K (see FIG. 1, 109 & 129), i.e., the input parameter is secret and is known only to Alice and Bob (where K can then be transformed into a secure authenticated session key). *Jablon* thus additionally fails to teach or suggest the subject matter of independent method claim 1 for this reason.

The Examiner (at pg. 3) cites *Patarin* in an effort to cure the shortcomings of *Jablon*; specifically, the failure to disclose "a chip and an application conducting the said authentication". Applicant disagrees with the Examiner's proffered analysis of *Patarin*. The combination of *Jablon* and *Patarin* fails to achieve the claimed invention, at least because (as discussed above) *Patarin* also fails to teach or suggest that a parameter x is previously calculated by the application and stored in a data memory of the hard-wired electronic chip, all before the hard-wired electronic chip is put into circulation, as recited in now-amended independent claims 1 and 32.

Patarin relates to a method and apparatus for authenticating a data carrier and discloses an authentication between a chip and an application loaded onto a memory. *Patarin* (col. 2, lines 19-21 and col. 3, line 46) describes the authentication of the chip by a terminal. *Patarin* (col. 2, lines 35-42) explains that a central computer 4 "includes processing circuits 5 and a memory 6 that communicate with one another and with an interface 7. Implanted in the memory 6 is the program of a cryptographic asymmetrical algorithm F, which in a manner known per se requires the use of a secret key Ks, also in memory, for enciphering a datum, while deciphering the datum requires the use of only a corresponding public key Kp". *Patarin* thus teaches that the memory of the central computer contains a cryptographic asymmetrical algorithm F and a secret key Ks, and that the memory of the terminal contains an algorithm G associated with the algorithm F and a public key Kp associated with the secret key Ks.

However, *Patarin* teaches not only authentication between a chip and an application that is loaded onto a memory but also that "it is desirable for neither the carrier [i.e., the chip] nor the associated terminal to contain a secret key, because such a key is vulnerable to being discovered by someone with an intent to commit fraud" (see col. 1, lines 32-35). *Patarin* thus teaches <u>away</u> from placing a secret key in a chip.

Patarin (col. 1, lines 25-35) explains that the "object of the invention is to propose a method of this type which employs the simplest possible means in the carrier itself and in an optional terminal of the distributor that is intended to cooperate with the carrier. In the case where the carrier is electronic, for example, it is desirable for it to be made up solely of a memory, without any associated calculation circuits, and for each memory to have the smallest possible size." The skilled person would have no reason to even consider the teachings of

Patarin were that person seeking, *arguendo*, to modify the structure of *Jablon* to achieve the method and device of independent claims 1 and 32, respectively.

Jablon describes methods for "two parties to use a small shared secret S to mutually authenticate one another over an insecure network" (see Abstract). As stated previously, *Patarin* specifically instructs that "[i]t is also desirable for neither the carrier nor the associated terminal to contain a secret key, because such a secret key is vulnerable to being discovered by someone with an intent to commit fraud". Clearly, *Patrin* teaches away from including a secret key in an electronic chip. Consequently, the skilled person would have no reason whatsoever to apply the disclosed EEPROM or other teachings of *Patrin* to the method of *Jablon*, absent impermissible hindsight analysis based on applicant's disclosure. *Jablon* teaches that Alice and Bob alone share knowledge of a secret password S. Therefore, absent an electronic chip in which to store the parameter x that is calculated by the application, before the hard-wired electronic chip is placed into circulation, and stored in a data memory of an electronic chip before the hard-wired electronic chip is placed into circulation, the deficiency of *Jablon* is apparent.

Moreover, independent claim 1 explicitly recites the step of "calculating, at the hard-wired electronic chip, a parameter y constituting an entire or a portion of the authentication value V via a serial function whose input parameters are at least the random number r specific to the transaction and a private key s belonging to an asymmetrical pair of keys". Independent claim 32 recites a corresponding feature. *Patarin* fails to teach or suggest this limitation, because the card in *Patarin* does not perform any mathematical calculations since it is merely comprised of memory (i.e., EEPROM 2)

The Examiner cites *Yeda* in an effort to cure the shortcomings of *Jablon* and *Patarin*; specifically, the failure to disclose "the producing of a pseudo-random number at application

prior to a transaction, calculating a corresponding parameter x at the application prior to the transaction, and the parameter being linked to pseudo-random number r by a mathematical relationship and storing of parameter x in memory of chip prior to transaction".

The combination of *Jablon*, *Patarin* and *Yeda*, however, in fact fails to achieve the claimed invention, at least because (as discussed above) *Patarin* additionally fails to teach or suggest that a parameter x is previously calculated by the application and is stored in a data memory of the electronic chip, all before the hard-wired electronic chip is placed into circulation, as recited in now-amended independent claims 1 and 32.

Yeda relates to a method and apparatus for implementing an identification and signature scheme (see Abstract). According to *Yeda*, the method and apparatus "enable an entity to generate proofs of identity and signatures of messages that everyone can verify but no one can forge" (see pg. 2, lines 12-13). Indeed, *Yeda* (Fig. 1, block 14) does disclose the production of a pseudo-random number. However, *Yeda* provides nothing to enable the skilled person to derive the method of independent claim 1 based on the production of this pseudo-random number. That is, *Yeda* fails to teach or suggest that a corresponding parameter x is calculated (i.e., at an application) before the hard-wired electronic chip is placed into circulation.

In *Yeda*, the corresponding parameter x is calculated at the chip (i.e., the prover of his identity) (see, e.g., pg. 2 lines 44-45, block 16 of Fig. 1) and is not calculated prior to the transaction within the meaning of now-amended claims 1 and 32. The flow diagram depicted in Fig. 1 of *Yeda* indicates that the parameter x is calculated after the random number r is chosen (see item 16, which intervenes to authenticate the chip in order to authorize a transaction). In applicant's method claim 1, the initial steps that occur prior to a transaction are separate from the steps that occur during the transaction.

Independent claims 1 and 32 have been amended to clarify the meaning of "prior to the transaction". Page 8, lines 14-16 of the specification provide a clarified definition of the meaning of this term, i.e., "before the hard-wired electronic chip is put into circulation". Thus, when it is said that the steps of producing the pseudo-random number r, calculating parameters x and storing x occur prior to the transaction, it means that these steps occur before the chip is put into circulation. In *Yeda*, two of these steps form part of the authentication process that is repeatedly performed, each time that the chip is required to prove its identity (see pg. 1, line 44).

In particular, *Yeda* (pg. 2, lines 44-45) explains that "[t]o prove his, hers or its identity, the entity chooses a random r in the range $0<r<n$, block 14, and sends $x=r^d$ (mod n) to the verifier, block 16 and line 18, where it is received by the verifier, block 20". *Yeda* thus clearly teaches that the parameter is not calculated before the chip is placed into circulation but, rather, the parameter is calculated after choosing the random number from an in-process or ongoing transaction.

Moreover, *Yeda* (pg. 3, lines 55-57) states that "[t]he size of the private key is about 4 kilobytes, but since each entity has to store only one such file, it can fit into almost any microcomputer based device (with the possible exception of a smart card)". This section of *Yeda* thus merely teaches that it — i.e., storage of the approximately 4 kilobyte private key — cannot fit into a smart card. This section of *Yeda* does not teach that a parameter x is stored in the memory of a hard-wired electronic chip.

In *Yeda*, the parameter is calculated by the prover (e.g., the chip) each time the chip is required to prove its identity via a mathematical expression $x=r^d$ $(mod\ n)$ (see, e.g., Fig. 1, block 16 (compute $x = r^d$ $(mod\ n)$). In the instant claimed invention, however, the parameter x is read from memory each time the chip is required to authenticate itself. This could only be possible if

the memory has been previously filled with the correct pseudo-random number r, in the manner recited in independent claims 1 and 32. As described at pg. 4, lines 1-14 of the instant specification, the claimed invention provides an asymmetrical method of authentication that can be implemented in a hard-wired electronic chip, such as a chip in which the surface area of the silicon is extremely small, where the calculation logic is reduced to extremely basic hard-wired operations.

The skilled person would have no reason whatsoever to apply the teachings of *Yeda* to the method resulting from the Examiner's proferred combination of *Jablon* and *Patrin*, absent impermissible hindsight analysis based on applicant's own disclosure. Lacking the storage of the parameter x that is calculated by the application prior to the transaction and that is stored in a data memory of an electronic chip, before the hard-wired electronic chip is placed into circulation, the deficiency of *Jablon* and *Patrin* is apparent.

The Examiner cites *Tanimoto* in an effort to cure the shortcomings of *Jablon*, *Patarin* and *Yeda*; specifically, the failure to disclose "the generator being located within the chip". The combination of *Jablon*, *Patarin*, *Yeda* and *Tanimoto*, however, fails to achieve the claimed invention.

Tanimoto "relates to an IC card and a microcomputer ... each of which includes a CPU and a memory..." (see paragraph [0001], lines 1-5). As explained at paragraph [0043], lines 4-5 of *Tanimoto*, the IC card comprises "an unillustrated one-chip microcomputer" and "[t]he IC card chip according to the present invention is basically identical in configuration to the microcomputer" (see paragraph [0045]). *Tanimoto* (paragraph [0049]) additionally explains that "[t]he CPU is configured in a manner similar to a so-called microcomputer". Fig. 2 of *Tanimoto* shows that the random number generator is part of the CPU.

In contrast, the claimed method and device encompass a hard-wired electronic logic chip. *Tanimoto* is not within in the same field of endeavour as applicant's claimed invention. The skilled person seeking to derive an authentication method for use with a hard-wired device would have no reason to consider the teachings of *Tanimoto*.

The microcomputer/CPU of *Tanimoto* is unsuitable for microprocessor-based cards. As explained at pg. 3, lines 2-8 of the instant specification, "[a]uthentication mechanisms of the above kind are well known in the art, but most of them demand calculation capacities at least equal to those of a microprocessor. Those mechanisms are therefore suitable for microprocessor-based cards, but are rarely if ever suitable for hard-wired logic chips, which have calculation capabilities that are much more rudimentary".

Page 4, lines 1-19 of the instant specification describes the need to integrate an active public key authentication mechanism into a hard-wired logic chip, "in particular in applications deploying a large number of chips, which is generally the case with applications using hard-wired logic chips because they are of very low cost. No such mechanism exists at present. The reason for this is that public key mechanisms generally require numerous operations on large numbers, and are therefore unsuited to integration in hard-wired logic chips, in which the surface area of the silicon is extremely small, and whose calculation logic is reduced to extremely basic hard-wired operations. These basic operations are generally effected serially, in the sense that the operands are introduced sequentially, bit by bit, and this progressively modifies the state of an internal register whose final value serves as a basis for calculating the result of the function. The claimed present invention relates to active public key authentication mechanisms that can be implemented in a hard-wired logic card".

Even assuming, *arguendo*, that the skilled person were to have a reason to consider the teachings of *Tanimoto*, *Tanimoto* teaches a random generator that is entirely different from the pseudo-random generator of claims 1 and 32 which generates a pseudo random number r which is linked to the number x by a mathematical relationship. *Tanimoto* teaches that an address A±S is obtained by adding a random number S to an initial address A..." (see paragraph [0093], lines 4-7). It would not have been obvious to derive applicant's claimed method and device from the combination of *Jablon*, *Patarin*, *Yeda* and *Tanimoto*. Independent claims 1 and 32 recite that the parameter x is previously – i.e., before the hard-wired electronic chip is put into circulation – calculated by the application and is stored in a data memory of the hard-wired electronic chip. *Yeda*, *Jablon*, *Patarin* and/or *Tanimoto* fail to teach or suggest such claimed features.

The Examiner additionally cites *Gentry* in an effort to cure the shortcomings of *Jablon*, *Patarin*, *Yeda* and *Tanimoto*; specifically, the failure to disclose "the use of public parameters exclusively to verify the authentication results", as recited in independent claim 32. The combination of *Jablon*, *Patarin*, *Yeda*, *Tanimoto* and/or *Gentry*, however, fails to achieve the claimed invention recited in independent claim 32.

Gentry relates to an authenticated ID-based cryptosystem including key agreement protocols that do not require key escrow. The Examiner in his proffered analysis asserts that *Gentry* discloses the use of public parameters exclusively to verify the authentication results, i.e., Fig. 5, item 516. Fig. 5 of *Gentry* "shows a flow diagram illustrating a method of determining a shared secret between two entities according to another presently preferred embodiment of the invention" (see paragraph [0017]).

Firstly, the processing associated with the flow diagram of *Gentry* does not correspond to "the use of public parameters exclusively to verify the authentication results". Secondly, *Gentry*

provides a description of Fig. 5 at paragraphs [0032] to [0039]. In these paragraphs, the only mention of "authentication" is provided at paragraph [0034], i.e., "[t]he second entity may then confirm that the first entity knows the non-interactive shared secret S_{AB} by confirming the message authentication code using the non-interactive shared secret S_{AB} as the key. Likewise, the second entity may prove...". There is no mention whatsoever of "the use of <u>public</u> parameters exclusively to verify the authentication results" as asserted. Moreover, the Examiner's proffered analysis also asserts that "[i]t would be obvious to one having ordinary skill in the art at the time of the invention of Jablon in order to have to be able to increase the number of processors added to the network as taught in Gentry see Fig. 6". The claimed invention is generally directed to calculating an authentication value V by a hard-wired electronic chip, and to verifying this authentication value V from exclusively public parameters. The teachings of *Gentry* have little to do with this claimed concept.

The combination of *Jablon*, *Patarin*, *Yeda* and *Gentry* thus fails to achieve the claimed invention, <u>at least</u> because (as discussed above) *Gentry* also fails to teach or suggest a parameter x that is previously calculated by the application and stored in a memory means of a hard-wired electronic chip, all before the hard-wired electronic chip is placed into circulation for use in a transaction. For at least this reason, the recitations of independent claim 32 are not rendered obvious by *Gentry* in combination with *Jablon*, *Patarin*, *Yeda* and/or *Tanimoto*.

Independent claims 1 and 32 are therefore <u>not</u> rendered obvious and unpatentable by the proffered combination of *Jablon*, *Patarin*, *Yeda, Tanimoto* and/or *Gentry*. Reconsideration and withdrawal of the rejection of claims 1 and 32 as unpatentable over the combination of *Jablon* with *Patarin*, *Yeda, Tanimoto* and/or *Gentry* under 35 U.S.C. §103 is accordingly deemed to be in order, and early notice to that effect is solicited.

Dependent Claims

In view of the patentability of independent claims 1 and 32 for at least the reasons presented above, each of dependent claims 2-31 is respectfully deemed to be patentable therewith over the prior art. Moreover, each of dependent claims 2-31 additionally includes features that serve to still further distinguish the claimed invention over the applied art.

Conclusion

Based on all of the above, applicant submits that the present application is now in full and proper condition for allowance. Prompt and favorable action to this effect, and early passage of the application to issue, are once more solicited.

Should the Examiner have any comments, questions, suggestions or objections, the Examiner is respectfully requested to telephone the undersigned in order to facilitate an early resolution of any outstanding issues.

It is believed that no additional fees or charges are required at this time in connection with the present application. However, if any such fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,
COHEN PONTANI LIEBERMAN & PAVANE LLP

By ______________________________

Lance J. Lieberman
Reg. No. 28,437
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: January 15, 2009